

Tesina di Sicurezza su reti EnCase

di Artuso Tullio, Carabetta Domenico, De Maio Giovanni

1

Sommario

- Computer Forensic
- Capisaldi per una corretta analisi
- EnCase
 - Overview
 - Preview
 - Acquisizione di prove
- Eliminazione sicura dei file
 - Eraser, tool di eliminazione sicura
 - Un esempio: Eraser vs. EnCase
- Limiti di EnCase
- Preservare la propria privacy

2

Computer Forensic (1)

- L'informatica forense comprende le attività di verifica dei supporti di memorizzazione dei dati e delle componenti informatiche, delle immagini, audio e video generate da computer, dei contenuti di archivi e basi dati e delle azioni svolte nelle reti telematiche.
- Scopo: conservare, identificare, acquisire, documentare e interpretare i dati presenti su un computer.
- Agisce **dopo** che un sistema informatico è stato violato per esaminare i reperti informatici in modo esaustivo, completo, accurato.

3

Computer Forensic (2)

Cos'è una prova digitale?

Insieme di informazioni e dati conservati o trasmessi dalle apparecchiature cosiddette digitali. Include ogni record, file, codice sorgente, programma, specifiche sul costruttore del dispositivo, e qualsiasi traccia residente sui supporti di memorizzazione.

4

Capisaldi per una corretta analisi

- *"se la macchina viene trovata spenta, deve rimanere tale"*, altrimenti accesa ma scollegata dalla rete.
- Durante l'analisi non deve essere introdotta alcuna alterazione ai dati residenti nel sistema, utilizzando tool per effettuare l'immagine dei supporti in modalità *"bit by bit"*.

5

Capisaldi per una corretta analisi(2)

- Usare particolari strumenti hardware che garantiscono che durante la fase di acquisizione non avvengano operazioni di scrittura sul media che si sta importando (ad esempio FastBloc).
- Nella formazione dell'immagine deve essere creata una "impronta" che contraddistingue in maniera univoca la prova digitale oggetto dell'analisi forense.

6

Capisaldi per una corretta analisi(3)

- L'impronta è creata con appositi algoritmi crittografici mediante una operazione di hashing che genera una sequenza unica di bit.
- Gli algoritmi più comunemente usati per la generazione di impronte hash sono SHA-1 e MD5 che, rispettivamente, creano una sequenza di 160 bit e 128 bit.

7

Capisaldi per una corretta analisi(4)

Tool per la Computer Forensic:

- EnCase
- SafeBack
- WinHex
- Autopsy & Sleuthkit
- Helix
- Foremost

8

EnCase

Overview

- È il prodotto commerciale più utilizzato per l'analisi delle tracce informatiche, destinato all'uso professionale ed investigativo.
- Infatti *"è il software più utilizzato nelle procedure di investigazione informatica da parte di organizzazioni governative e forze dell'ordine a livello mondiale"*.

9

EnCase

Overview (2)

- Compie l'acquisizione producendo un esatto duplicato binario di dati del media originale.
- Se utilizzato con le dovute accortenze (le prove sulla macchina in esame non vengono mai alterate) e utilizzando specifici hardware, come ad esempio FastBloc, è completamente non "invasivo".

10

EnCase

Modalità Preview

- Consente all'investigatore di visionare in anteprima il contenuto del drive in esame prima di effettuare una acquisizione.
- Vantaggi: risulta la funzione più veloce e facile da effettuare. Inoltre un investigatore può effettuare un'analisi preliminare di un drive prima di acquisirlo.
- Svantaggi: Se non accompagnato da hardware write blocking comporta l'inevitabile alterazione di alcuni dati relativi al drive esaminato, come la data di accesso all'hardware stesso, qualora vengano "aperti" o modificati i file al suo interno.

11

EnCase

Acquisizione di prove

EnCase mette a disposizione diverse modalità di acquisizione...

- **Parallel Port Cable Acquisition:** usata quando nessun'altro metodo di Acquisition o di Preview funziona. In genere usata per notebook con hard disk difficilmente rimovibili, oppure per acquisire un hardware con tecnologia RAID.
- **Network Cable Acquisition:** consente di acquisire o vedere in anteprima il media su cui si vuole investigare via rete e solo mediante cavo Crossover.

12

EnCase

Acquisizione di prove (2)

EnCase mette a disposizione diverse modalità di acquisizione...

- **Drive to Drive Acquisition:** l'hardware da esaminare viene fisicamente collegato al computer dell'investigatore cosicché i supporti (Storage e Subject IDE drives) sono collegati alla stessa scheda madre. Con questa modalità il computer da esaminare non è in "Server Mode", quindi non viene usato l'EnCase Boot Disk.
- **FastBloc Windows Acquisition:** FastBloc è un dispositivo che offre un ottimo livello di prestazione. Si tratta di uno dei più avanzati hardware write-blocking che protegge il dispositivo di memorizzazione collegato da qualsiasi tipo di scrittura (accidentale o volontaria) e permette quindi l'acquisizione del media sorgente in Windows in maniera estremamente sicura e veloce.

13

EnCase

Acquisizione di prove (3)

EnCase mette a disposizione diverse modalità di acquisizione...

- **Acquiring Removable Media:** in questa modalità è possibile acquisire i dati da supporti removibili come Zip Disk, Jaz Disk, Floppy Disk, Superdisk, CD-ROM, CD-R, CD-RW...
- **Acquiring Palm PDA:** questa modalità consente di reperire informazioni da palmari.

14

Eliminazione sicura dei file

Con i comandi:

- "del", in ambiente DOS
- "svuota cestino", in ambiente Windows
- "rm", in ambiente Linux

in realtà non cancelliamo affatto il contenuto del file vero e proprio: vengono cancellate le intestazioni del file dall'elenco interno utilizzato dal file system.

Di fatto, però, il vecchio contenuto rimane scritto su disco fino a quando non viene sostituito da nuovi dati che ne vanno ad occupare l'esatta posizione.

Perciò i file "cancellati" possono in realtà continuare a essere disponibili.

15

Eliminazione sicura dei file (2)

EnCase vs. Eraser

- Eraser è un tool di sicurezza avanzato che permette di cancellare in modo permanente ed irrecuperabile qualunque dato memorizzato su disco utilizzando tecniche evolute di wiping.
- È un programma freeware e open source.
- In grado di sovrascrivere anche le aree libere del disco fisso in modo tale che neppure i file che erano memorizzati in tali parti del disco possano essere recuperati.

16

Eliminazione sicura dei file (3)

EnCase vs. Eraser

Modalità di cancellazione opzionali:

- **Pseudorandom data:** sovrascrive una volta sola il file con dati casuali.
- **US DoD 5220.22-M (8-306. /E):** è uno standard consigliato dal Dipartimento di Sicurezza Statunitense, che prevede la sovrascrittura del file per tre volte, con particolari sequenze di sovrascrittura (ad esempio si sostituisce il file prima con una sequenza di 00000000 poi di 11111111 poi con una sequenza di dati casuali).
- **US DoD 5220.22-M (8-306. /E, C and E):** prevede la sovrascrittura del file per sette volte.
- **Gutmann:** prevede una sovrascrittura con ben 35 passaggi, sempre seguendo uno schema che alterna determinate sequenze di 00000000, di 11111111 e di dati casuali.

17

Eliminazione sicura dei file (4)

EnCase vs. Eraser

Un esempio:

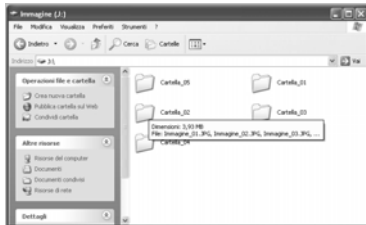
- Analizziamo in dettaglio EnCase recuperando file cancellati con Eraser v. 5.6.
- Confrontiamo tale procedura con il recupero dei file eliminati svuotando il cestino.

18

Eliminazione sicura dei file (5)

EnCase vs. Eraser

Creiamo cinque cartelle, e in ognuna di esse, andiamo ad inserire dieci immagini.

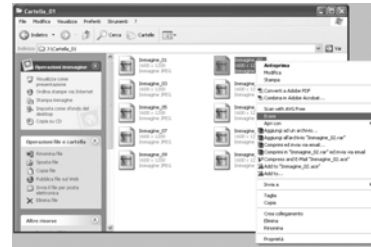


19

Eliminazione sicura dei file (6)

EnCase vs. Eraser

Eliminiamo i file della Cartella_01 utilizzando Eraser (usando Gutmann come algoritmo di cancellazione).



20

Eliminazione sicura dei file (7)

EnCase vs. Eraser

Cancelliamo i file della Cartella_02 con Eraser ma, questa volta, deseleggiamo le opzioni "Cluster Tite Area" e "File names" dal menù "Options".

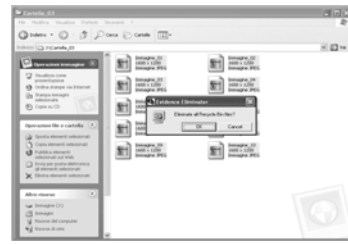


21

Eliminazione sicura dei file (8)

EnCase vs. Eraser

Per la Cartella_03 cancelliamo i file usando un altro tool di rimozione sicura, *Evidence Eliminator v5.0*.

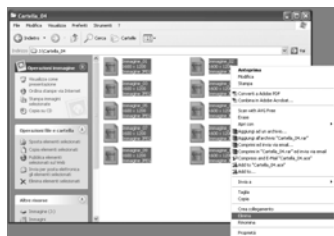


22

Eliminazione sicura dei file (9)

EnCase vs. Eraser

Cancelliamo i file della Cartella_04 semplicemente spostandoli nel cestino e successivamente lo svuotiamo.



23

Eliminazione sicura dei file (10)

EnCase vs. Eraser

Lasciamo invariato il contenuto della Cartella_05.



24

Eliminazione sicura dei file (10)

EnCase vs. Eraser

Recuperiamo i file usando EnCase
Osserviamo il seguente risultato...

Cartella_01: immagini e i nomi dei file sono completamente irrecuperabili.

Cartella_02: deselezionando le opzioni "*cluster tip area*" e "*file names*" vengono recuperati soltanto i nomi dei file ma le immagini vengono perse.

Cartella_03: alcune immagini sono completamente recuperabili, di altre sono recuperabili solo i nomi.

Cartella_04: i file sono completamente recuperabili (nome, immagine e tutti i dettagli sui file).

Cartella_05: tutto è rimasto invariato.

25

Limiti di EnCase

- Guidance Software non rende visibile il codice sorgente del programma.
- Manca trasparenza, indipendenza e verificabilità delle tecnologie usate dal tool.
- Il numero di file system supportati è limitato (ignora reiserfs, ext3, jfs, ufs, hfs, hfs+, veritas).

26

Limiti di EnCase (2)

- Riconosce un limitato insieme di formati di file.
- Al fine di migliorare l'autenticità delle prove è necessario utilizzare un ulteriore strumento di validazione, il *time-stamping*.
- Il costo del software è elevato.

27

Preservare la propria privacy

- In alcuni casi un computer è potenzialmente violabile da utenti curiosi o malintenzionati.
- Queste azioni, se effettuate, potrebbero alterare, cancellare o modificare in maniera decisiva le prove da recuperare.

Come difendersi?

28

Preservare la propria privacy (2)

Come difendersi?

- L'utilizzare *data compression*, deframmentazione di dischi e programmi di ottimizzazione.
- Download di file di grosse dimensioni, che sovrascrivono rapidamente i cluster "non allocati".
- Usare programmi che sovrascrivono settori di disco con stringhe di "0" (ad esempio con la funzione *Erase unused space* di Eraser).

29

Preservare la propria privacy (3)

Come difendersi?

- Installare di nuovo software applicativo.
- Configurare sistemi operativi e partizioni.
- Cancellare i "*Temporary Internet Files*", "*browser history*" e "*cookie*".
- Modificare il time clock del computer.

30